RCMA FY04 Commanding Officer Conference

PKI 101 - Introduction to DoD PKI

CTR2 Dumm

Training Agenda

- Security Benefits of PKI
- Encryption Overview
- What is a Public Key Infrastructure?
- DoD PKI Roles and Responsibilities
- What REDCOM N6 is doing?
- Software Certificate vs. CAC
- Timeline
- Questions?

Why do we need PKI?

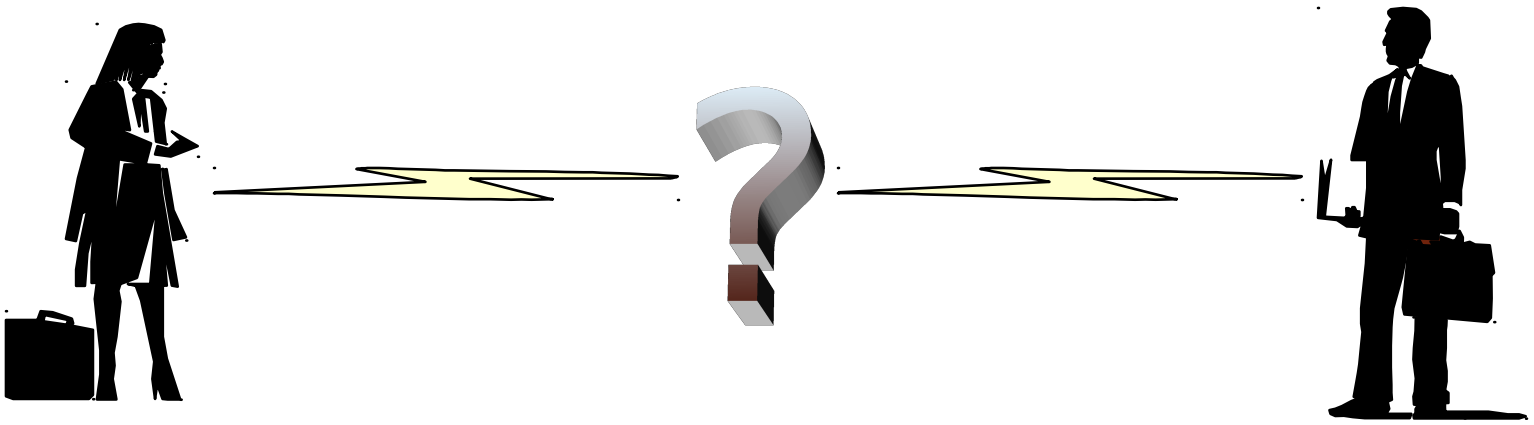
***First*, DoD has mandated that all personnel who access DoD systems must use PKI for all non-public email and web transactions by 1 April 2**

***Second*, PKI improves the NAVY force protecti posture by ensuring the integrity & confident of our email & web transactions.**

Remember, NIPRNET-based transactions are not secure DISA reports foreign entities have accessed and change US government email!

The Need for Trust

How can Alice and Bob trust each other over a netw
if they have never met and there is no “face-to-face
verification procedure?

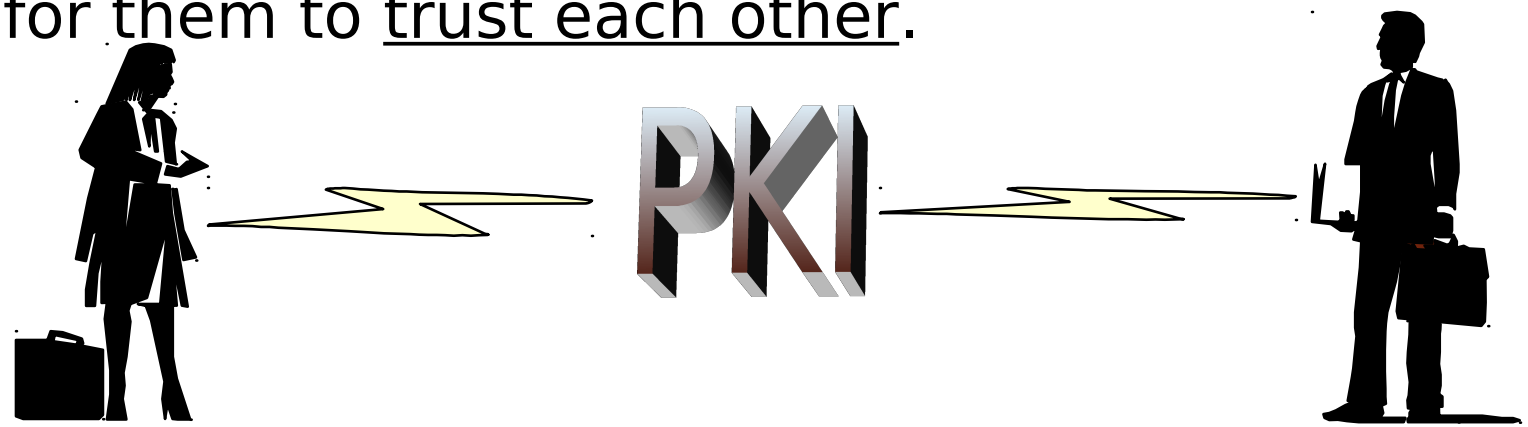


Alice

Bob

Establishing Trust

An infrastructure of trusted third parties is put in place to distribute trust between end-users. This infrastructure verifies that both Alice and Bob are who they say they are. If they trust the infrastructure, then the infrastructure can vouch for them to trust each other.



What is A Public Key Infrastructure?

- **PKI**

  A *Public Key Infrastructure* is the framework and services that provide for the generation, distribution, control, tracking and destruction of public key certificates. The purpose of a PKI is to manage keys and certificates in a way whereby an organization can maintain a *trustworthy networking environment*. PKI enables the use of encryption, digital signature, and access authentication services in a consistent manner across a wide variety of applications.

- **DoD PKI**

  DoD's implementation of a Public Key Infrastructure encompassing the entire Department of Defense.

What is A Public Key Infrastructure?

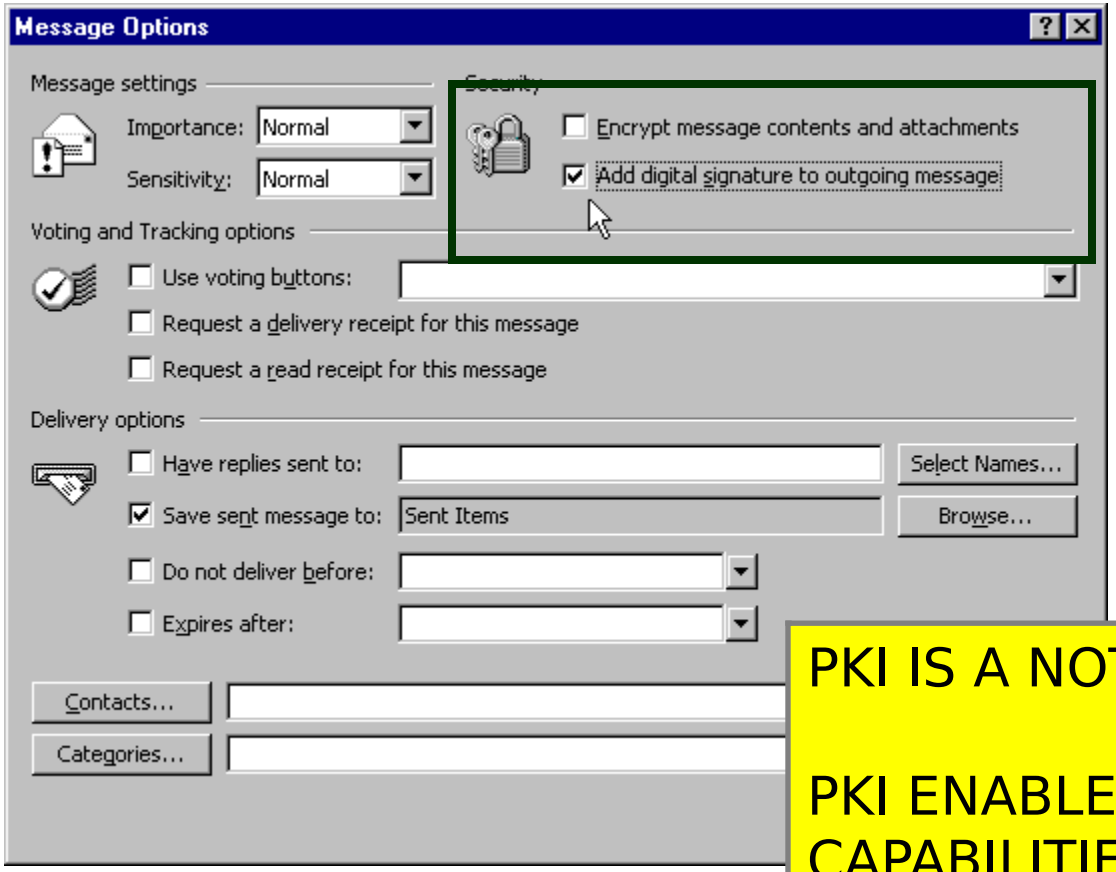
IN THE DOD PKI, EVERY USER WILL GET THREE CERTIFICATES:

“IDENTITY” CERTIFICATE: USED TO IDENTIFY YOU TO A WEBSITE, A NETWORK, A COMPUTER, OR A PKI-ENABLED SYSTEM, SUCH AS NAVSUP SECURE INTRANET.

“EMAIL SIGNATURE” CERTIFICATE: USED FOR SIGNING EMAIL.

“EMAIL ENCRYPTION” CERTIFICATE: USED TO ENCRYPT EMAIL.

What is A Public Key Infrastructure?



MS Outlook – Options Dialog box

The PKI part

PKI IS A NOT A NEW APPLICATION.

PKI ENABLES THE SECURITY CAPABILITIES OF YOUR EXISTING EMAIL AND WEB APPLICATIONS.

Security Benefits of PKI

- **Authentication**

  Assures that a person or system is exactly who or what they claim to be

- **Data Integrity**

  Assures that transmitted data has not been altered (intentional or accidental)

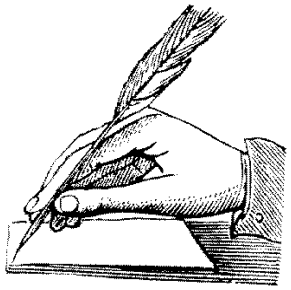
- **Non-repudiation**

  Protects against a person denying later that a communication or transaction took place as recorded

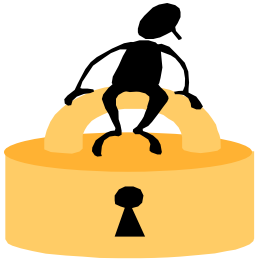
- **Confidentiality**

  Protects against the disclosure of information to unauthorized users. Encryption is typically used to assure confidentiality when information is transmitted over networks.

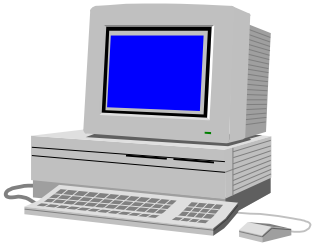
With PKI you can…



1. <u>DIGITALLY "SIGN" EMAIL</u>. THIS ENSURES THAT YOUR EMAIL WASN'T CHANGED IN TRANSIT. FOR MANY TRANSACTIONS, PKI ELIMINATES THE NEED TO MAIL DOCUMENTS.



2. <u>ENCRYPT EMAIL</u>. YOU CAN USE PKI TO PROTECT SENSITIVE BUT UNCLASSIFIED MATERIAL, SUCH AS MEDICAL & FINANCIAL DATA.



3. <u>ACCESS PKI-ENABLED WEB SITES AND SYSTEMS</u>. PKI REPLACES LESS SECURE AUTHENTICATION MECHANISMS, SUCH AS PASSWORDS AND DOMAIN FILTERING (.MIL, .GOV).

DoD PKI Roles and Responsibilities

Software Certificates	Hardware Certificates	Role Description
Certificate Authority (CA)	Certificate Authority (CA)	Creates and signs public key certificates
Registration Authority (RA)	DMDC Verification Process	Authorizes creation of a certificate and provides information to the CA
Local Registration Authority (LRA)	DEERS/RAPIDS Verification Officer (VO)	Verifies users' identity and issues certificates
End User (Subscriber)	End User (Subscriber)	Uses keys in applications; ultimate authority to verify that the entity in the transaction has proper credentials
Repository (Directory)	Repository (Directory)	Device used to store and retrieve public key

Certificate Revocation

- **There are many reasons to revoke a certificate (before it expires automatically)**
  - Change in status
    - User may no longer be authorized to sign on behalf of the organization
    - Certificate might contain obsolete information (e.g. the employer, job title, name or email address has changed)
  - Lost CAC
  - Compromise of a portion of the certificate chain higher up in the hierarchy

Why do we need PKI?

***First*, DoD has mandated that all personnel who access DoD systems must use PKI for all non-public email and web transactions by April 200**

***Second*, PKI improves the NAVY force protecti posture by ensuring the integrity & confident of our email & web transactions.**

Remember, NIPRNET-based transactions are not secure DISA reports foreign entities have accessed and change US government email!

DoD PKI Policies

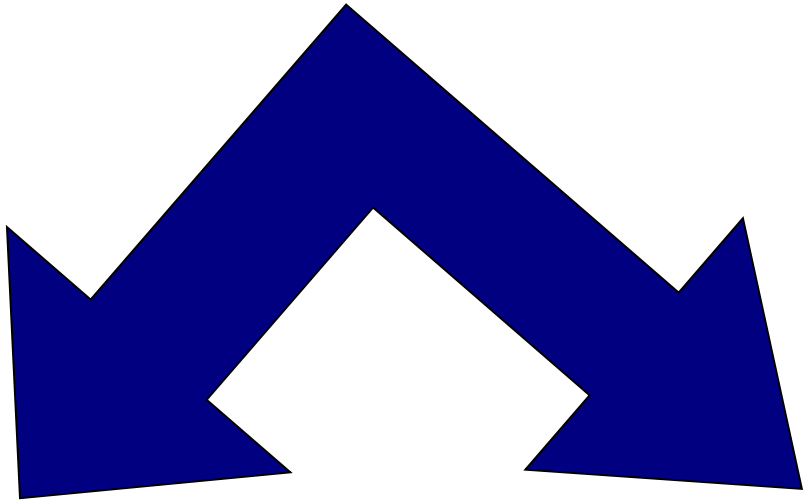
- All electronic mail sent within DoD will be digitally signed by Apr. 2004 (per OSD guidance)
- DoD components are encouraged to encrypt email within the DoD
- All DoD personnel will be issued CAC cards as a replacement for DoD ID cards
- The certificates used for signature and encryption will be standardized DoD PKI certificates (no other Certificate Authorities will be recognized)

Impact on the Naval Reserve

- All personnel will be required to use PKI to access Navy websites such as DFAS and BUPERS
- CNET's courses website is the one Navy website currently using PKI for authentication and encryption
- If we do not encourage our personnel to use PKI they will not have access to critical career information
- DOD Certificates and NMCI certificates are not the same

What REDCOM Mid-Atlantic N6 is Doing

N6 is taking a two prong approach to make this happen



CAC Card Readers

Soft Certificate

CAC Card Readers

- **Distribution is complete**
  - All Reserve Centers have 75
    - 50 USB and 25 Serial Readers per center
    - With the tools available to order additional readers.
  - A few bugs to work out
    - There are some problems with software compatibility
    - Above average technical knowledge required for installation
    - Incompatible USB drivers with some Operating System configurations (Windows ME, XP Home and 2000)

Soft Certificates

- **This is the alternative solution that REDCOM N6 is pursuing**
  - Soft (i.e., software) certificates are being issued by the LRA (Local Release Authority) at the Washington Navy Yard
  - They will be issued on diskette to all users who are unable to use the CAC Card reader
  - They are password protected and can be installed on the members home machine with little technical knowledge.

Software Certificate vs. CAC

Attribute	Hardware (CAC)	Software (Floppy)
Security	• Adversary needs physical possession • PIN is enforced • Only one copy of private key • All encryption/decryption performed on the CAC • CAC locks after 3 unsuccessful tries	• Adversary could more easily steal private key without user's knowledge because it is stored on each user's computers • PIN isn't enforced • Multiple copies of private key • All encryption/decryption performed on the computer • No lockout
Portability	• CAC goes with you, but you need a card reader on each machine you use	• Must be installed on every computer you use, but no card reader is needed

Timeline for Implementation

Task	REDCOM N6 Deadline	Reserve Center Deadline
All CAC Card Readers are issued to Reservists	Completed	31 JAN 04
CAC Card Readers are installed	15 DEC 03	27 FEB 04
Software Certifications are issued	16 JAN 04	13 FEB 04
Software Certifications are installed	05 FEB 04	5 MAR 04

Additional Information

- DoD PKI
  - DoD PKI PMO https://iase.disa.mil/PKI/
  - Navy PKI Help Desk https://infosec.navy.mil/PKI
    1-800-304-4636
  - For detailed hardware or software certificate installation instructions, see system administrator training
- DoD CAC
  - DoD Access Card Office (ACO) RAPIDS Schedule
    http://www.dmdc.osd.mil/smartcard/
    (703) 696-7396

Conclusion

Questions?

Or

Contact:

Scott Day N6 Department Head (202) 433-2327 or
IT1 Williams (202) 433-6208